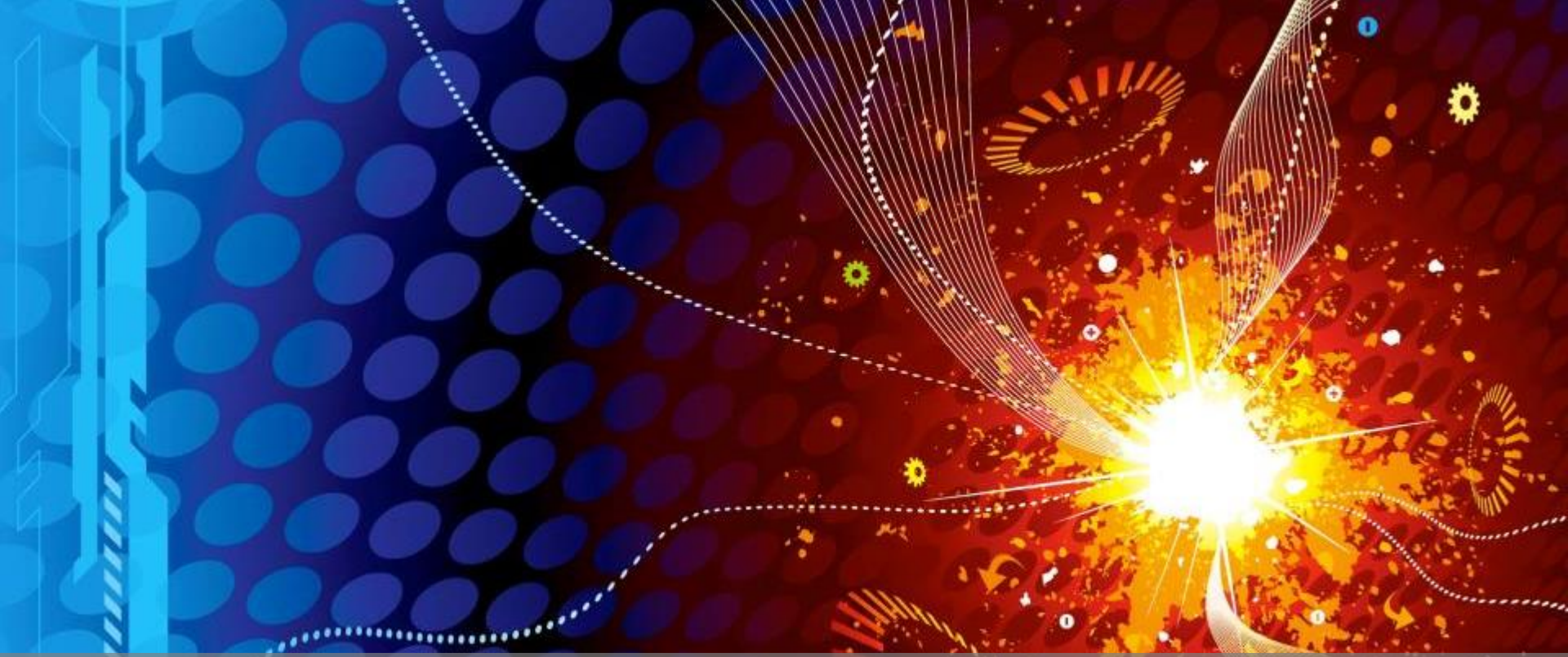


Centre for Risk Studies Research Showcase 13 January 2015

Session 1: Cambridge Risk Framework

Developing Frameworks for Managing Cyber Catastrophe Risk

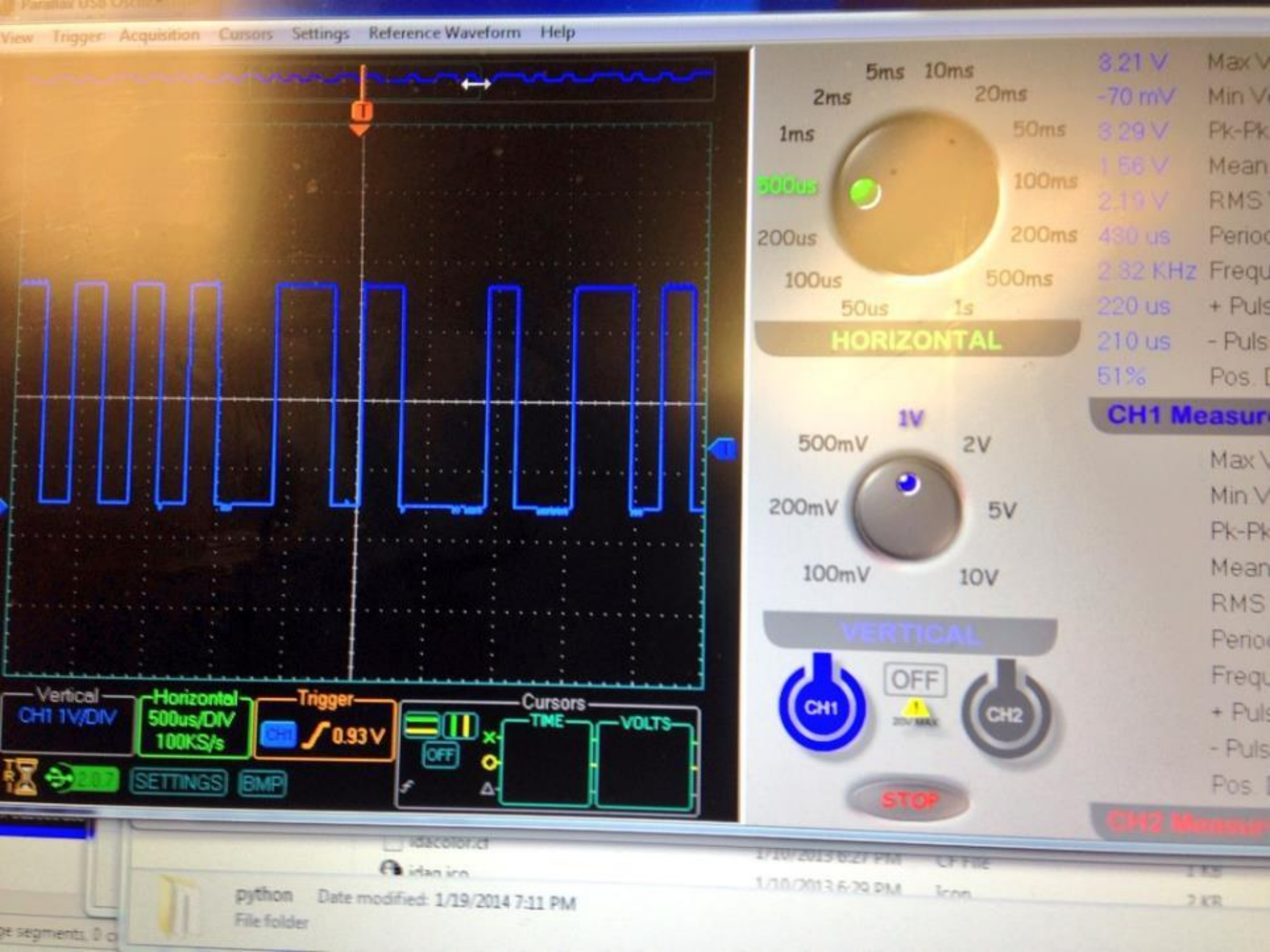
Centre for Risk Studies

UNIVERSITY OF CAMBRIDGE Judge Business School

Éireann Leverett

~~Senior Risk Researcher~~ Ex-Pirate

Centre for Risk Studies


View Trigger Acquisition Cursors Settings Reference Waveform Help
5ms 10ms
2ms 20ms
1ms 50ms
500us 100ms
200us 200ms
100us 500ms
50us 1s
HORIZONTAL
1V
500mV 2V
200mV 5V
100mV 10V
VERTICAL
CH1
OFF
CH2
STOP
3.21 V
-70 mV
3.29 V
1.56 V
2.19 V
430 us
2.32 KHz
220 us
210 us
51%
CH1 Measure
Vertical
CH1 1V/DIV
Horizontal
500us/DIV
100KS/s
Trigger
0.93 V
Cursors
TIME
VOLTS
SETTINGS
BMP
python
Date modified: 1/19/2014 7:11 PM
File folder


НОМЕР
КОЛОДЦА
ПОВЫШЕНИЕ Р
ПОНИЖЕНИЕ Р
К.З.
ОБРЫВ
ЦПРП
УКДМ
N 082
1992Г
КОНТРОЛЬ
ПР. 0,5А
=220В
ВКЛ
СЕТЬ


SECURITY
SENTRON
PAC2400
SIMATIC S7-1500
Modular Controller
SCALANCE
X310FE
SITOP
Smart
SINAMICS G120
GP Drive
SIMATIC ET200S
Distributed I/O


C4T

Why isn't Cyber Solved Yet?

- Misaligned incentives
  - Who do you pay to hack you?
  - What do you do when they succeed?
- Race to the bottom
  - Time to market pressure for software, skip security!
- Invisible failures
  - Last time someone failed to log into your account?
- Tragedy of the commons
  - Who polices bandwidth usage? DDoS reflectors? Routing?
- No price discrimination on security/privacy
  - You chose your car because of the locks right?
  - Laptop? Operating System? Email provider?

Why is Cyber a Different/Similar Risk?

- It is a network of networks
- Physical laws (and metaphors) don't apply
- Man Made Peril
- Frequency & Severity poorly understood
- Rapidly changing trends
- Was cyber's effect on the global economy:
  - Revolutionary?
  - Disruptive?
- Why wouldn't the solutions be:
  - Revolutionary.
  - Disruptive.

Towards a Framework

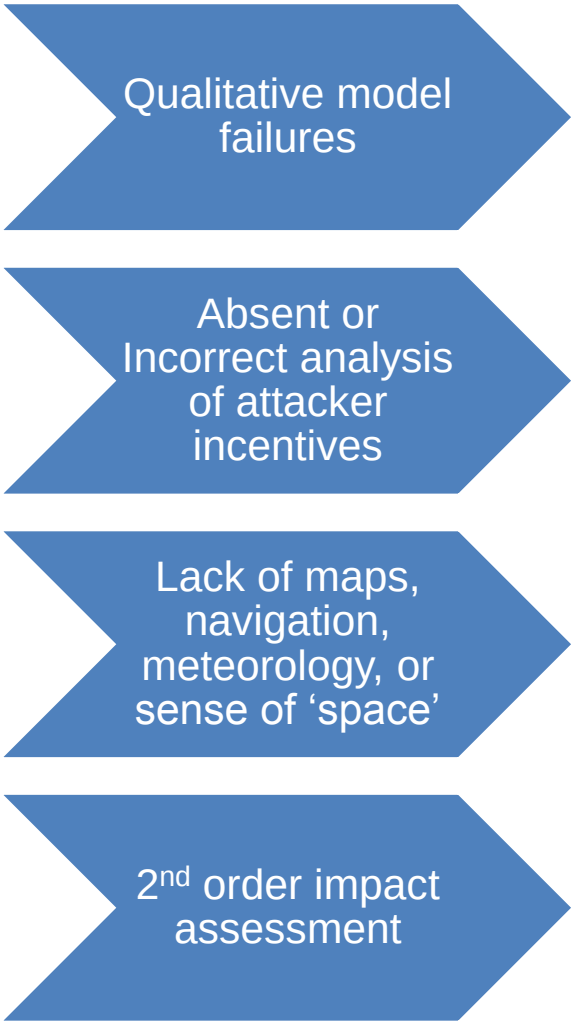
- Mapping the ‘shape’ of cyber
- Managing latent legacy risk
- Adopting less risk
- Handling a crisis as a business or a nation
- Finding the systemic, endemic, risks
- Building risk management consortiums
- What is the data interface between re-insurers and tech-security companies?
- How do you measure vulnerability?

Adopt a metric: Leverett-Wightman Cost

We published a sample opportunity cost of finding a particular type of vulnerable device online in 2012

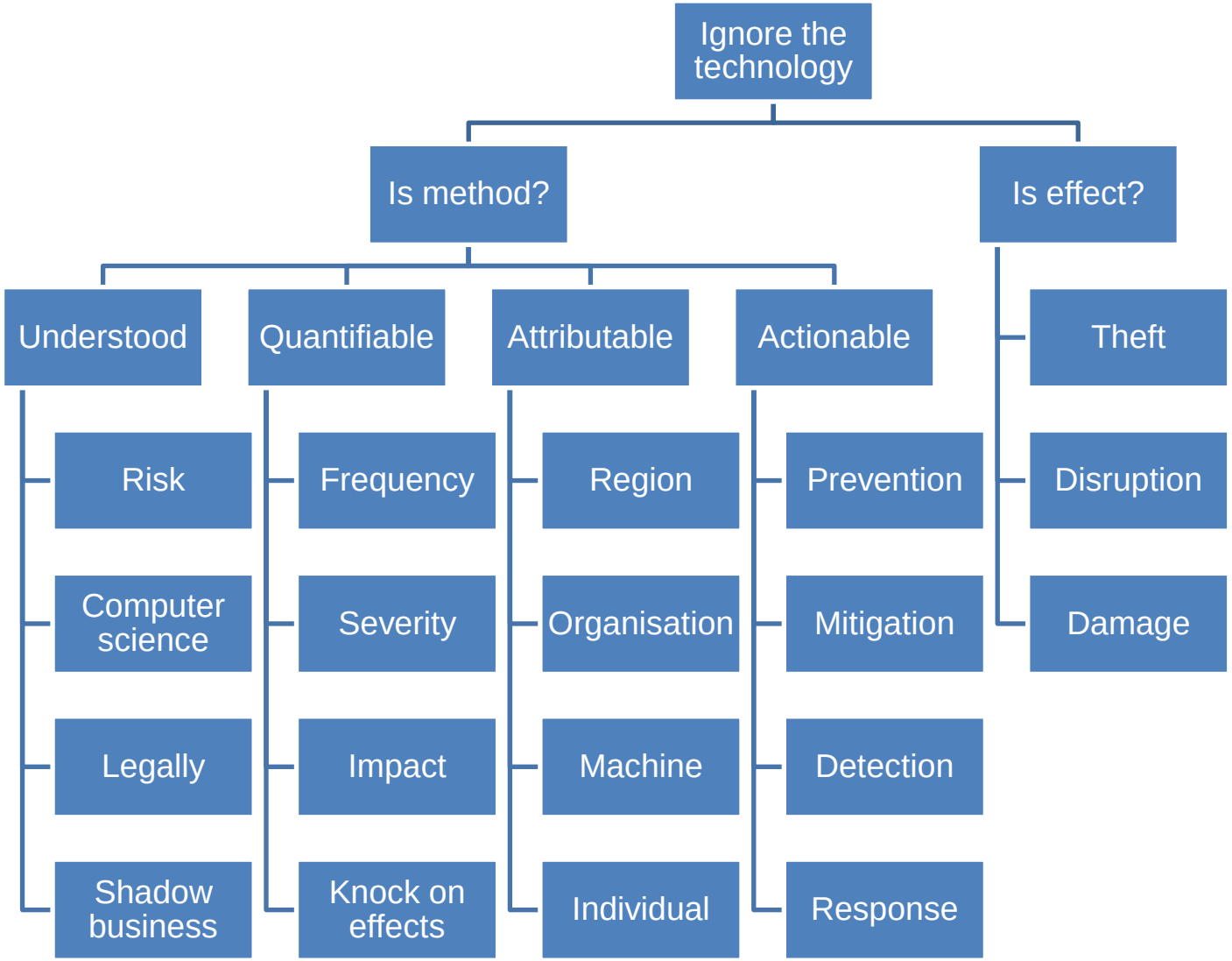
1. This metric is methodology and technology independent.
2. As costs for parallelisation fall this is incorporated into the metric.
3. As newer, faster scanners (such as ZMAP) are developed this is also included in the metric.
4. The density of vulnerability across a network space is factored into the metric.
5. Partial scans can still be used for metrics.
6. We understand the cost to attackers of finding opportunistic targets.
7. We understand the low cost to this methodology of defending.
8. We understand the change over time in the lifecycle of exposure and vulnerability.
9. It naturally translates a technical problem into an economic one ready for debate and policy discussion.

Catastrophe Models

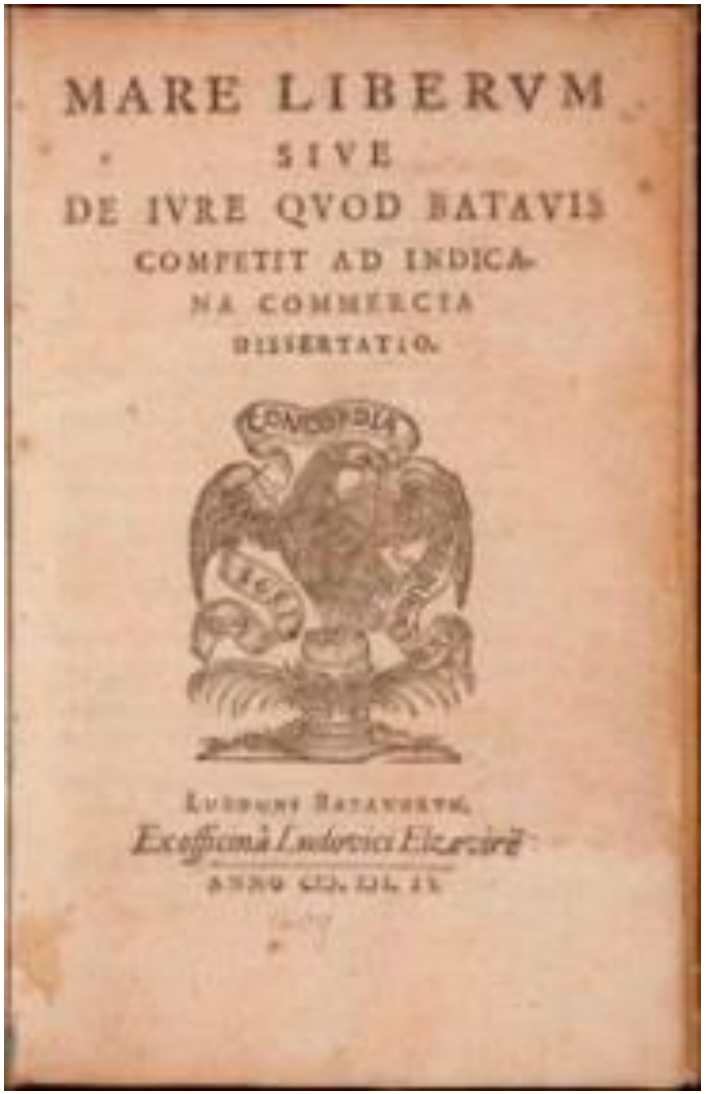


- A Risk Assessment Model for Cyber Attacks on Information Systems
  - [Patel & Zaveri 2010]
- Identifying, Understanding, and Analysing Critical Infrastructure Interdependencies
  - [Rinaldi, Peerenboom, Kelly 2001]
- Modelling interdependencies between the electricity and information infrastructures
  - [Laprie, Kanoun, Kaâniche 2007]
- Towards modelling the impact of cyber attacks on a smart grid
  - [Kundur, Feng, Mashayekh, Liu, Zourntos and Butler-Purry 2008]

A Cyber Crisis Management Framework

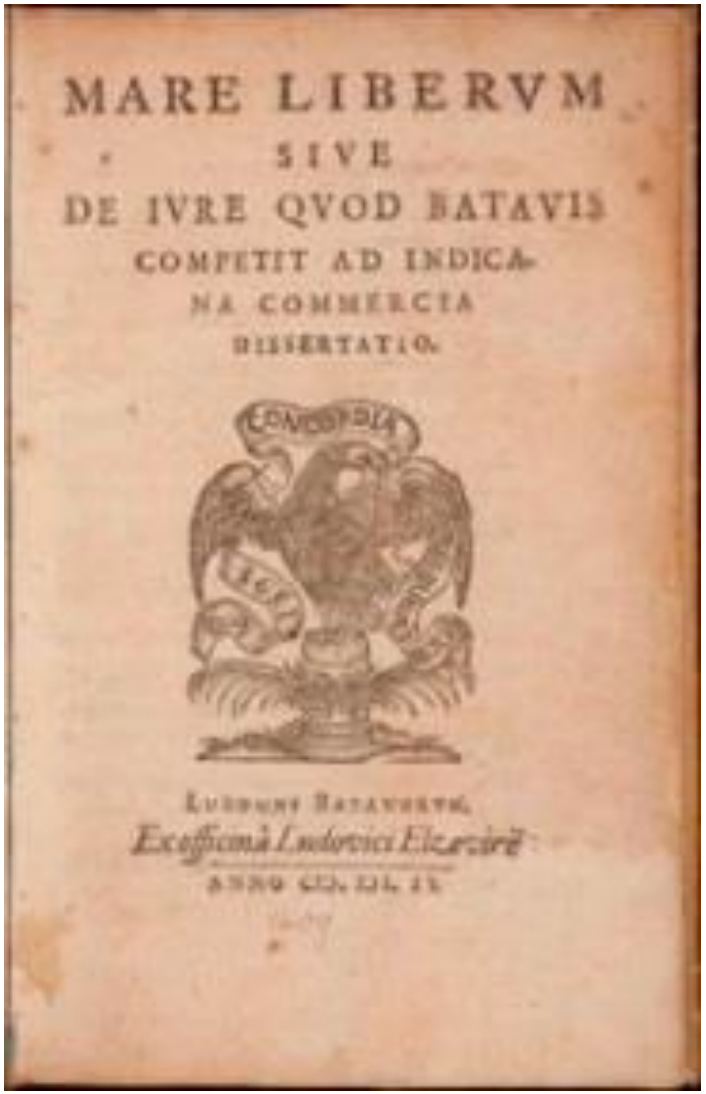


Has Civilisation Been Here Before?



- The golden age of piracy
  - 1480-1800
- A contested sea
  - Disruption
  - Damage
  - Theft
- Rapid changes in frequency and severity
- Information Asymmetry
- Companies caught between nations

We Solved This Before



- Nation State
- Organised Crime
- Hacktivist
- Jurisdiction
- Attribution
- Legal Uncertainty
- Companies as a battle ground for nations
- Trade risk
- Misunderstood attacker incentives

A Map, a Watch, a Sextant, and a Shipping Forecast.

Solutions are definitely not ‘local’.

Not all solutions are technical.

Risk management of a technical commons.

Whose job is it?

How do we manage ’the interim period’?

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School